

# Herausforderungen der Cyberkriminologie

Von Dr. Thomas-Gabriel Rüdiger, Oranienburg\*

---

## 1 Digitaler Transformationsprozess

---



Kaum eine Entwicklung in den letzten Jahrzehnten hat vermutlich solch ein Potential grundlegende gesellschaftliche Transformationsprozesse auszulösen wie die allgegenwärtige Digitalisierung. Dabei nur von Digitalisierung im Sinne einer Nutzung technischer Möglichkeiten und Geräte auszugehen, geht hierbei nicht weit genug. Vielmehr umfasst die Digitalisierung auch die Etablierung eines globalen digitalen Raumes – besser vermutlich einer globalen digitalen Sphäre – der grenzfreien Interaktion und Kommunikation zwischen Menschen auf der ganzen Welt und aus jedem Kulturkreis. Diese Kommunikation und Interaktion findet gegenwärtig vor allem über sog. Soziale Medien statt, diese stellen dabei eine Art Metabegriff für unterschiedlichste Formen von Programmen dar. Am ehesten kann man sich hierunter onlinebasierte Programme vorstellen, die eine Vernetzung und Kommunikation zwischen den Nutzern zu lassen. Diese Definition erfasst dann sowohl die klassische Vorstellung Sozialer Netzwerke wie Facebook, Instagram, TikTok oder Twitter, geht über Messenger wie Whatsapp, Telegram oder Kik und reicht bis zu dem hier klar dazu zählenden Bereich der Onlinespiele (Bayerl und Rüdiger 2017, 921 ff). Diese Medien sind schon lange kein Randphänomen mehr, sondern Menschen halten sich in diesen genauso selbstverständlich auf wie im öffentlichen Straßenverkehr.

---

## 2 Mediennutzung in Deutschland

---

Knapp 94% aller Deutschen ab 14 Jahren sollen in irgendeiner Form in diesem digitalen Raum unterwegs sein. Bei den 14- bis 49-jährigen sollen es 100% sein, bei den bis 69-jährigen 95% und bei den über 77-jährigen noch immer 77% (Krupp und Bellut 2021, S. 6). Täglich nutzen sogar 76% der Deutschen ab 14 Jahren das Internet, was in etwa 54 Millionen Menschen entspricht (Beisch und Koch 2021, S. 488). Bei der Internetnutzung spielen auch in Deutschland die Sozialen Medien eine wichtige Rolle, diese werden von 59% der Bevölkerung ab 14 Jahren genutzt. Allein WhatsApp wird von 70% der Bevölkerung täglich genutzt. Bei der Nutzung Sozialer Medien zeichnet sich zudem eine gewisse Alterskluft ab, so nutzen in der Alterskategorie der 14- bis 29-jährigen 66% täglich Soziale Medien, bei den 50- bis 69-jährigen hingegen nur 17%. Als verbreitetes klassisches Soziales Medium, hat Instagram, das von 18% der Befragten täglich genutzt wird, mittlerweile Facebook abgelöst, dass nur von 15% am Tag noch angesteuert wird. Trotz der medialen Präsenz von Twitter nutzen es nur 2% der Befragten, genauso viele wie Twitch, eine Plattform auf der primär Gamingssessions gestreamt werden (Beisch und Koch 2021, S. 498). Alleine die 14- bis 29-jährigen nutzen Onlinemedien mittlerweile 269 Minuten also fast 5 Stunden am Tag (Beisch und Koch 2021, S. 491). Dabei ist diese Entwicklung nicht nur auf Jugendliche und Erwachsene beschränkt. Bereits im Jahr 2014 nutzten 25% der Kinder von 6 bis 7 Jahren zumindest selten das Internet. Mittlerweile sind es in dieser Alterskategorie 34%, bei den 8- bis 9-jährigen sind es sogar 60% und bei den 12- bis 13-jährigen kann mit 97% von einer Vollabdeckung gesprochen werden. Im Durchschnitt nutzen 82% der Kinder unter 14 Jahren mehrmals das Internet in der Woche (Feierabend et al. 2020, S. 37). Auch in diesen Altersstufen ist WhatsApp das wichtigste Soziale Medium und wird von 53% der Kinder täglich und 68% zumindest mehrmals in der Woche genutzt. Weitere 59% nutzen Youtube, 20% Instagram und Snapchat (Feierabend et al. 2020, S. 39). Nach der „Mediensuchtstudie 2020“ der DAK ist die Nutzungszeit Sozialer Medien bei Minderjährigen um 66% von 115 auf 192 Minuten täglich angestiegen (Bodanowitz und Scharf 2020, S. 10). Es erscheint daher nicht unrealistisch anzunehmen, dass viele Menschen über alle Altersgrenzen hinweg spätestens im Rahmen der Corona-Einschränkungen täglich mehr Zeit in der digitalen Sphäre verbringen als im gesamten physischen Straßenverkehr.

---

### 3 Cyberkriminologische Betrachtung eines globalen digitalen Raums

---

Ein Grundgedanke der Kriminalwissenschaft ist, dass Kriminalität und normenabweichendes Verhalten immer aus einer Interaktion und Kommunikation zwischen Menschen entsteht. Das gleiche gilt im Umkehrschluss auch für die Normengenese und Formen der Normdurchsetzung. Eine Gemeinschaft einigt sich durch unterschiedliche Prozesse auf gemeinsame Verhaltensweisen und darauf, dass diese dann bei Bruch der Regeln auch durchgesetzt und geahndet werden oder im Falle von einer Neubetrachtung zu Legalisierungen führen. Hierfür braucht es einerseits das Verständnis, dass man sich als eine Gemeinschaft definiert und damit die Regeln akzeptiert. Andererseits müssen die Gruppenmitglieder zumindest rudimentär wissen welchen Regeln sie konkret unterliegen. Eine Thematik die sich auch im sog. Bestimmtheitsgebot als Ausformung des Art. 20 Abs. 3 GG widerspiegelt. Ein hierzu notwendiges und gleichzeitig naheliegendes Grundkonstrukt ist es, dass ein Mensch weiß in welchem Land er sich aufhält und welchen Regeln er damit auch unterliegt. Dies wird faktisch auch dadurch gewährleistet, dass ein Mensch – je nach Konstellation – physische Landesgrenzen überqueren muss und dadurch ahnt, dass er neuen Regeln unterliegt. Auch die Kriminalwissenschaft hat hierbei die leichte Tendenz, die Betrachtung von Kriminalität auf das jeweilige nationale Verständnis von unterschiedlichen Deliktsformen auszurichten.

Das Konzept, dass Menschen wissen sie befinden sich physisch an einem Ort und unterliegen dessen Gesetzen, findet aber seine Grenze im digitalen Raum. Denn das Kennzeichen vor allem von Sozialen Medien, Onlinespielen und Co. ist gerade die Schaffung einer prinzipiell globalen und grenzfreien Vernetzungs- und Kommunikationssphäre. Diese Globalität des digitalen Raums kennt aber im Gegenzug keine sichtbaren virtuellen Landesgrenzen in sozialen Medien und im Internet im Allgemeinen, die man überschreiten könnte. Dies bedeutet faktisch auch, dass die moralischen und damit auch rechtlichen Vorstellungen unterschiedlichster Länder in derselben Sphäre aufeinandertreffen. Genauer die Menschen, die durch diese Vorstellungen geprägt wurden, nun aber ihre eigenen Vorstellungen in diesem Raum transportieren, ohne das klar definiert ist, wer welchem Recht in welchem Moment eigentlich unterliegt. Was in dem einen Land in den Sozialen Medien strafbar sein könnte, könnte in dem anderen Land, vielleicht überhaupt nicht gesetzlich geahndet werden.

Als ein Beispiel was damit gemeint ist könnte eventuell die Einordnung sog. „Posingbilder“, also Abbildungen von unnatürlichen Körperhaltungen von Kindern in teils bekleideten oder unbekleideten Zustand, als kinderpornographische Inhalte herangezogen werden. Hierunter können beispielsweise entsprechende Inhalte von Kindern in Unterwäsche fallen. Spätestens seit der Reform des § 184b StGB im Jahr 2014/2015 sind solche Abbildungen in § 184b Abs. 1 Nr. 1 StGB als strafbar einzuordnen. Für einige immer wieder überraschend sind kinder- oder auch jugendpornographische Inhalte nicht nur auf das Darknet beschränkt. Nach einer Analyse im Rahmen des Projekts Arachnid des Canadian Centre for Child Protection (CSAM) waren 97% der festgestellten Missbrauchsabbildungen im Clearweb abgelegt und nicht im Darknet (CSAM 2021, S. 2). In letzter Zeit wird immer klarer, dass Missbrauchsabbildungen auch in Sozialen Medien zu finden und über Messenger geteilt werden. In den USA können Missbrauchsabbildungen, auf die Nutzer stoßen, über die Meldefunktion „CyberTipline“ des National Center for Missing & Exploited Children (NCMEC) gemeldet werden, die nach einer Prüfung die Informationen an Sicherheitsbehörden auch in Deutschland weitermelden. Im Jahr 2020 gab es hierüber etwa 22 Millionen Meldungen, etwa 100.000 davon entfielen auf Deutschland (NCMEC 2021b). Von diesen 22 Millionen Meldungen betrafen knapp 90% die Social Media Programme von Meta (früher Facebook), also Facebook, Instagram und WhatsApp. Die Problematik von Missbrauchsabbildungen in Sozialen Medien greift daher auch die polizeiliche Prävention durch entsprechende Kampagnen auf (ProPK 2021).

Hier schließt sich nun der gedankliche Kreis. Es gibt nämlich keine weltweit absolut gültige Definition von kinderpornographischen Inhalten. Das bedeutet, dass beispielhaft ein Nutzer auf einer Social Media Plattform ein problematisches Bild eines Kindes sehen könnte, dass in Deutschland z.B. als Posingbild qualifiziert wird, aber in dem Land in dem der Nutzer das hochgeladen hat, vielleicht gar keine strafrechtliche Relevanz hat. Dadurch kann theoretisch die Situation eintreten, dass Nutzer aus dem einen Land sich fragen, warum offenbar andere völlig unproblematische aus ihrer Sicht strafbare Handlungen posten können. Wessen strafrechtliche Wertevorstellung sollen dann in Sozialen Medien eigentlich greifen?



---

## 4 Ein globales digitales Strafrecht?

---

Faktisch bräuchte ein globaler digitaler Raum auch ein gemeinsames globales Strafrecht, dass eine weitestgehend akzeptierte Wertevorstellung umfasst. Die Forderung eines globalen Strafrechts für den digitalen Raum ist dabei nicht neu, auch wenn es offenbar nicht mehr sehr präsent ist. Bereits im Jahr 2000 hat der damalige deutsche Innenminister Schily im Rahmen von Angriffen durch den Email Wurm „ILOVEYOU“ ein globales Strafrecht für das Internet gefordert und schon zu dem Zeitpunkt betont, dass das Internet kein rechtsfreier Raum sei (Kuri 2000). Erst jüngst hat sich die mangelnde Durchsetzungsmöglichkeiten eines nationalen Staates auf den global agierenden Messenger „Telegram“ mit Sitz in Dubai gezeigt (Hoven 2021). Dieser reagiert schlicht nicht auf Anfragen des deutschen Staates im Zusammenhang mit der Bekämpfung von Hasskriminalität bzw. der Erfassung als Soziales Netzwerk nach dem Netzwerkdurchsetzungsgesetz (NetzDG) und zeigt sich auch nicht sehr kooperativ in der Zusammenarbeit mit deutschen Sicherheitsbehörden (Metzger 2021). Dies zeigt auch im Umkehrschluss auf, dass die Durchsetzung nationaler Regeln doch stark auf ein „good will“ der beteiligten Firmen angewiesen ist, wenn das aber nicht vorhanden ist wird es schwierig. Gleichzeitig nutzen aber bereits 2019 etwa 8 Millionen Deutsche auch Telegram (Mehner 2021). Dabei werden die Telegram Nutzer hier auch mit problematischen Inhalten konfrontiert, sehen gleichzeitig aber, dass gerade die Sicherheitsbehörden offenbar kaum in der Lage sind hier Regeln durchzusetzen. Während die Menschen also physisch in dem einen Land sind und eigentlich wissen, dass sie dessen Regeln unterliegen, sind sie im virtuellen gleichzeitig in einer eigenständigen Sphäre unterwegs, in welcher der Staat wesentlich geringere Durchsetzungsmöglichkeit hat oder die vorhandenen nur selten anwendet.

---

## 5 Normalität digitaler Delikte?

---

Neben einer Vielzahl an Auswirkungen dieser Globalität auf die gefühlte und tatsächliche Strafverfolgungswahrscheinlichkeit im digitalen Raum, soll hier ein besonderer Punkt angesprochen werden. Die nur geringe Durchsetzung von nationalen Regeln, wird jedem Nutzer vermutlich nicht selten bei seiner täglichen Internetnutzung präsentiert. Bereits ein Blick in den Spamordner, konfrontiert viele Nutzer tagtäglich mit versuchten Betrugsdelikten in Form von Phishing-E-mails. Eine Erhebung von Statista im Auftrag der Internet-Sicherheitsfirma GData ergab, dass 31% der Internetnutzer angaben, bereits Opfer von einer Phishing-E-mail geworden zu sein (GData 2021). Eine Studie der Bitkom ergab, dass sich die Anzahl der Nutzer, die noch nie Erfahrungen mit Kriminalität im Netz gemacht haben, seit 2018 von damals noch 40% auf nur noch 21% im Jahr 2021 fast halbiert hat (Bitkom 2021). Nach derselben Studie stieg zudem die Konfrontation mit digitaler Hasskriminalität an. Gaben 2020 nur 6% der Nutzer an damit selbst Erfahrung gemacht zu haben, waren es 2021 bereits 14% (Bitkom 2021). Besonders bedenklich sind in diesem Zusammenhang auch die Ergebnisse der JIM-Studie 2021, nach der 58% der befragten Minderjährigen von 12 bis 19 Jahren in einem Monat mit Hassbotschaften und 56% mit „extremen politischen Ansichten“ konfrontiert wurden (Feierabend et al. 2021, S. 62). Gleiches gilt auch für den Bereich der sexuellen Übergriffe, denen sich Minderjährige im Netz ausgesetzt sehen. Hier sticht vor allem Cybergrooming, also die onlinebasierte Anbahnung oder Intensivierung eines sexuellen Kindesmissbrauchs,

hervor (Bruhn et al. 2021, S. 120; Rüdiger 2020). Eine repräsentative Studie der Landesanstalt für Medien NRW kommt für das Jahr 2021 zu dem Ergebnis, dass knapp jeder vierte befragte Minderjährige onlinebasierte Kontaktabbahnungen durch Erwachsene mit dem Ziel eines Treffens erlebt hat. Konkret berichteten 9% der 8- bis 9-jährigen, 14% der 10- bis 12-jährigen und 25% der 13- bis 15-jährigen sowie knapp 40% der 16- bis 18-jährigen von solchen Kontaktabbahnungen (Nennstiel und Isenberg 2021). Ähnlich viele Minderjährige haben auch erlebt, dass Erwachsene ihnen im Netz im Austausch für Bilder von ihnen beispielhaft virtuelle Items in Onlinespielen versprochen haben (Nennstiel und Isenberg 2021, S. 20). Auch wenn juristisch Cybergrooming unter § 176a Abs. 1 Nr. 3 und § 176b Abs. 1 StGB nur Kinder als Betroffene erfasst, sind dies aber Zahlen, die sich bereits länger in unterschiedlichen Studien mit ähnlichen Konfrontationshöhen widerspiegeln und es deutet viel auf eine erlebte Normalität dieser Übergriffe im Netz hin (Rüdiger 2020). Man kann es auch anders formulieren, bereits seit einiger Zeit werden Minderjährige und damit mittlerweile auch junge Erwachsene zumindest teilsozialisiert in einem digitalen Raum, der offenbar geprägt ist von diesem Erleben der Konfrontation mit Kriminalität und Normenbrüchen. Sie sind quasi mit einer Art Unrechtskultur im digitalen Raum aufgewachsen (Rüdiger 2019). Was dies eigentlich für Auswirkungen auf diese Generationen hatte und hat, ist bisher überraschenderweise weitestgehend unerforscht.

---

## **6 Hat die digitale Kriminalitätstransparenz Auswirkungen auf das Sicherheitsgefühl der Menschen?**

---

All diese Deliktsformen haben zumindest eine Besonderheit sie machen Kriminalität im Netz für die Nutzer transparent und zeigen gleichzeitig, dass offenbar viele TäterInnen keine allzu große Angst vor einer Strafverfolgung haben müssen, sonst würden sie ja vermutlich nicht mit so viele Delikten stetig konfrontiert werden. Kriminalität im Netz wird also in einer Form für die Nutzer wahrnehmbar, wie sie es aus dem physischen Raum in dieser Omnipräsenz nicht kennen. Das Ergebnis hiervon ist offenbar das Gefühl, dass der Rechtsstaat im Netz weitestgehend versagt. Im Rahmen der bereits zitierten Bitkom Studie stieg der Anteil derjenigen die mehr Angst vor Kriminalität im Netz, als vor solcher im analogen Raum haben, von 39% im Jahr 2020 auf 48% im Jahr 2021 (Bitkom 2021). Man könnte es vermutlich auch anders formulieren, die Frage, ob Menschen Kriminalitätsfurcht haben, scheint immer mehr von ihrem Onlineerleben beeinflusst zu werden. Demgemäß glauben auch nur 6%, dass „Internetkriminalität in der öffentlichen Debatte übertrieben dargestellt“ werde (Bitkom 2021). Vielleicht ist diese Situation auch eine der Erklärungen dafür, warum seit Jahren eine Diskrepanz zwischen polizeilich registrierten Anzeigen (die an die Staatsanwaltschaft abgegeben werden) (PKS) und dem Sicherheitsgefühl der Menschen in Deutschland besteht (vgl. hierzu u.a. Bruhn et al. 2021). Nach einer Studie der Konrad Adenauer Stiftung gehen Ende 2021 52% der dort Befragten davon aus, dass Kriminalität in Deutschland in den letzten fünf Jahren etwas (36%) bis stark (26%) zugenommen hat (Konrad Adenauer Stiftung 2021). Teilweise scheint in der Innenpolitik ein Art Unverständnis zu herrschen, warum die Leute eigentlich eine so „falsche Wahrnehmung“ von Kriminalität haben, wenn diese doch vermeintlich zurückgeht. Tatsächlich verzeichnet die PKS seit dem Jahr 2015 einen kontinuierlichen Rückgang von 6.330.649 Fällen auf 5.310.621 Fälle im Jahr 2020, was einer Verminderung von etwas über 16% der angezeigten Handlungen entspricht (BMI 2021b). Diese ist insofern überraschend, da im selben Zeitraum die Bevölkerungszahl Deutschlands mit etwa 83,1 Millionen Einwohnern im Jahr 2021 stetig angestiegen ist und mittlerweile einen Höchststand erreicht hat (Statistisches Bundesamt 2021). Dieser Deliktsrückgang gilt jedoch nicht für Delikte im Zusammenhang mit dem Tatmittel Internet. Bereits im ersten Halbjahr 2021 sollen so viele kinderpornographische Delikte bei der Polizei zur Kenntnis gekommen sein wie die gesamte Polizeiliche Kriminalstatistik (PKS) 2020 zu registrieren hatte (Welle 2021). Dabei hatte die PKS 2020 mit 18.761 Fällen bereits einen signifikanten Anstieg, um knapp 55% im Verhältnis zu 2019 mit 12.262 Fällen, zu verzeichnen (BMI 2021b). Sollte sich diese Entwicklung tatsächlich bewahrheiten, würden sich die Fallzahlen in der PKS 2022 bei etwa 40.000 Fällen eingepegeln. Noch im Jahr 2015 lagen die Fallzahlen bei lediglich 5.687, dies würde, wenn es so eintritt, also einen Anstieg von etwa 600% seit dem bedeuten. Entsprechend warnt der Präsident des Bundeskriminalamts auch davor, dass „die deutliche Zunahme solcher Fälle die Polizei zunehmend an Kapazitätsgrenzen bringen (wird) ...“ (Welle 2021). Dabei muss davon ausgegangen werden, dass diese Entwicklung vornehmlich durch internetbasierte Modi Operandi getragen wird. Von den 18.761 Fällen in der PKS 2020 wurden 12.516 über das Tatmittel Internet begangen, auch der Anstieg der internetbasierten Delikte entspricht 56% und ähnelt damit dem Anstieg der Gesamtzahlen in diesem Bereich (BMI 2021a). Dieser Anstieg ist sicherlich auch auf die oben beschriebenen automatischen Meldungen über die Cybertipline von NCMEC zurückzuführen (NCMEC 2021a).

---

## **7 Braucht es im Netz eine nutzerfreundliche Anzeigemöglichkeit?**

---

Zumindest teilweise kann der Rückgang der PKS Fallzahlen in den letzten Jahren offenbar damit erklärt werden, dass die Menschen im analogen öffentlichen Raum immer weniger Zeit verbringen. Damit sinkt auch das Risiko, dass hier Kriminalität, bspw. Straßenkriminalität, begangen werden kann. Faktisch auch weil potentielle TäterInnen und Opfer weniger Möglichkeiten

haben aufeinanderzutreffen. Parallel verbringen die Menschen aber immer mehr Zeit im digitalen Raum und werden hier einerseits mit Kriminalität konfrontiert und es bieten sich ihnen andererseits auch Möglichkeiten zu einfachen Tatbegehungen, dank einer niedrigen Tatbegehungsschwelle. Ein Grundproblem hierbei ist, dass die sog. Dunkelzifferrelation, also das Verhältnis zwischen einem Delikt im Hell- und Dunkelfeld, wesentlich ungünstiger ist als bei klassischen analogen Delikten (Rüdiger 2021). Das Ergebnis ist, dass das Helfeld analoger Delikte sinkt, das Dunkelfeld digitaler Delikte aber im Gegenzug nur minimal aufgehellt wird. Diese Situation aufzubrechen, würde eine Erhöhung der Anzeigewahrscheinlichkeit erfordern. Dies kann entweder dadurch geschehen, dass den Nutzern verdeutlicht wird, wann es sich um Straftaten handelt und dass sich eine Anzeige auch lohnt. Dies könnte beispielhaft mit niederschweligen Anzeigemöglichkeiten im Netz ermöglicht werden. So ist es wenig verständlich, warum in einem globalen digitalen Raum jedes Bundesland eine eigene Internet- oder Onlinewache unterhalten muss, anstatt eine Art Single Point of Contact Möglichkeit für Anzeigen über digitale Wege anzubieten. Auch kann hinterfragt werden, ob die Anzeigemöglichkeit über diese virtuellen Wachen „nutzerfreundlich“ gestaltet oder doch eher kompliziert vom Mechanismus her sind. So fehlt es faktisch an einer Art rund um die Uhr besetzten virtuellen Anzeigeraum, bei dem auch Onlinenutzer direkt mit Polizeiangehörigen per Chat kommunizieren können. Also ähnlich wie es auf den meisten Polizeiwachen ja möglich ist. Auch existieren keine sich speziell an die Bedürfnisse von Kindern ausgerichtete Kontaktmöglichkeiten im digitalen Raum zur Polizei. Beispielhaft eine Kinderonlinewache, die rund um die Uhr mit Fachpersonal aus verschiedenen Bereichen besetzt ist und eine Chatmöglichkeit für Kindern gerade in Zeiten von Homeschooling bietet. Selbst viele offizielle polizeiliche Social Media Accounts beispielhaft auf Instagram, die für eine Kontaktaufnahme durch Nutzer aber vor allem Minderjährige in Frage kämen, beinhalten in ihren Profilen den Hinweis „keine Anzeigen“ (@Polizeiberlin 2021), „keine Anzeigenerstattung & DM“ [gemeint ist Kontaktmöglichkeit über „direct messenger“] (@bremenpolizei 2021), oder gleich den Hinweis „Nachrichten werden nicht gelesen!“ (@polizeisachsen 2021). Hintergrund dieser Hinweise und einer offenbar vorhandenen Form von Kommunikationsunlust der Sicherheitsbehörden im digitalen Raum ist vermutlich eine gewisse Skepsis vor einer Überforderung mit der Sichtung von Anfragen und den damit einhergehenden Personalbedarf, ausgelöst auch aus der weitestgehenden absoluten Gültigkeit des Legalitätsprinzips. Welche Außenwirkung dies aber z.B. auf Minderjährige haben könnte, die gerade in ihrer digitalen Lebenssphäre Hilfe suchen, wurde noch nicht hinterfragt. Im Rahmen der oben bereits zitierten Studie zu Cybergrooming wurde auch herausgearbeitet, dass lediglich 9,6% der betroffenen Minderjährigen das Verhalten bei der Polizei zur Anzeige bringen würde (Nennstiel und Isenberg 2021, S. 34). Umso wichtiger wäre es, die Kommunikationsschwelle mit der Polizei und damit auch die Möglichkeit der Anzeigenerstattung allgemein im Netz niedrig zu halten, oder anders ausgedrückt nutzerfreundlich.

Eine weitere Möglichkeit wäre, dass die Polizei selbst im Netz aktive zufällige Präsenz zeigt, also auf eine Art virtuelle Streife geht und dabei die dort selbst festgestellten Straftaten zur Anzeige bringt. Teilweise finden solche Maßnahmen im Sinne der sog. „anlassunabhängigen Internetrecherche“ zumindest punktuell, wenn auch verdeckt, statt (LKA NRW 2021). Eine belastbare Aussage über die Anzahl von deutschen Polizeiangehörigen, die in dieser Form im Netz dienstlich auf Streife gehen ist für die letzten Jahre nicht eruierbar, es lässt sich aber vermuten, dass diese nicht allzu hoch sein dürfte. Schilderungen deuten zudem daraufhin, dass wenn sie durchgeführt werden, solche Streifen nicht als Hauptaufgabe gesehen werden, sondern offenbar nur als eine Art „Nebenbei“. Im Kontext einer TV-Dokumentation zu den Auswirkungen der Aufstufung des § 184b StGB zu einem Verbrechenstatbestand, äußerten Kriminalbeamte, dass sie vor allem durch die Zunahme an kinderpornographischen Medien gar nicht mehr in der Lage sind gegen das Phänomen Cybergrooming aktiv selbst vorzugehen: „Dazu haben wir keine Zeit. Das bearbeiten wir im Zweifel erst, wenn tatsächlich schon etwas passiert ist“ (NDR 2021). Ein proaktives Vorgehen über sog. polizeiliche Scheinkindoperationen – wenn sich also Polizisten im Netz als Kinder ausgeben, um TäterInnen zu überführen (Rüdiger 2020) – um die Taten im Vorfeld zu verhindern, findet demnach weitestgehend gar nicht statt. Im übertragenen Sinne bedeutet es, dass der Fensterwurf nicht verhindert wird, sondern nur die Scherben aufgekehrt werden. Konkret vorzuwerfen ist dies nicht, scheint es doch ein Symptom eines strukturellen Problems der Adaption der Mechanismen des digitalen Raums durch die Sicherheitsbehörden zu sein.

---

## 8 Es braucht eine echte digitale Polizeistrategie

---

In Kombination mit der Warnung des BKA-Präsidenten vor einer Überforderung der Kapazitäten der Sicherheitsbehörden bei kinderpornographischen Inhalten, den hohen Fallzahlen bei digitalen Delikten im Allgemeinen und Schilderungen wie in dem vorhergehenden Beispiel entsteht das Bild, dass die Sicherheitsbehörden gegenwärtig nur gering aktiv sein können, um selbst Straftaten aufzudecken und in der Folge dann auch verfolgen zu müssen. Denn je mehr die Sicherheitsbehörden investieren würden, umso mehr Anzeigen würde es – auch ganz in Anlehnung nach dem Lüchow-Dannenberg Syndrom – geben. Eine Situation die innenpolitisch auch ausgehalten werden müsste. Dazu kommt, dass die bisherigen Formen von Präsenz bei virtuellen Streifen für die Nutzer weitestgehend nicht erkennbar sind, die generalpräventive Wirkung, die beispielsweise durch Uniformen und Streifenwagen im Straßenverkehr entstehen, können so offenbar gar nicht erst im digitalen Raum greifen. Ohne diese Wirkung aber, könnten die Sicherheitsbehörden vermutlich noch so viel Personal im Netz einsetzen, ohne einen allzu großen Effekt zu haben. Denn dieser Raum besteht ja nicht nur aus deutschen Nutzern, sondern faktisch aus den weltweiten Internetnutzern. Dies zeigt sich gegenwärtig offenbar bei der digitalen Hasskriminalität, bei der sich trotz aller polizeilichen und kriminalpolitischen Maßnahmen die Situation, wie die dargestellte Studienlage zeigt, noch weiter verschlechtert hat.

Im digitalen Raum scheint eine Situation eingetreten zu sein, nach der Kriminalität so sichtbar wird, dass das von Popitz beschriebene Prinzip der „Präventivwirkung des Nichtwissens“, nach der das Vorhandensein eines Dunkelfelds einen normenstabilisierenden Faktor einnimmt, durchbrochen zu sein scheint (Rüdiger 2021). Das bedeutet, dass sich die Sicherheitsbehörden grundlegenden auch strukturellen Herausforderungen stellen müssen. Welche Aufgabe können sie wie in einem globalen digitalen Raum mit weltweiten Internetnutzern wahrnehmen, in dem Kriminalität für die Menschen transparent und wahrnehmbar wird, und gleichzeitig die Mechanismen der Normenkontrolle (noch) kein Gegengewicht bilden. Hier gibt es keine einfachen Antworten nach dem Motto, ich bilde mal X „Cybercops“ aus oder engagiere einige ExpertInnen. Wenn die Sicherheitsbehörden ihre Funktion als Normenkontrolle im Netz nicht vollends an große digitale Plattformen wie Meta verlieren wollen, dann braucht es jetzt die Entwicklung einer echten zukunfts tragenden Polizeistrategie für einen digitalen Raum, die sich als Teil einer grundlegenden kriminalpolitischen, eventuell sogar globalen Neuausrichtung sieht. Diese Strategie darf dann auch nicht davor zurückscheuen, Fragen wie die Relevanz einer auf örtlicher Zuständigkeit basierenden polizeilichen Gefahrenabwehr im digitalen Raum, die absolute Gültigkeit des Legalitätsprinzips vor dem Hintergrund der Masse der digitalen Delikte und der damit erschwerten Schwerpunktsetzung, oder auch die nach der Sinnhaftigkeit einer föderativen Polizeistruktur in diesem Raum, zu stellen.

Seit etwa 10 Jahren war diese Entwicklung absehbar (Denef und Rüdiger 2013), es sollte nicht ein weiteres Jahrzehnt dauern bis man erkennt, dass es sich nicht einfach nur um „neue“ Kriminalitätsphänomene, sondern um einen gänzlich eigenständigen polizeilichen Einsatzraum handelt, der in einer Wechselwirkung mit dem analogen steht, aber dennoch auch etwas eigenständiges ist. Wenn es schon nicht bei den vergangenen Generationen geglückt ist, sollten doch zukünftige Generationen davor bewahrt werden, in einer Art anomischen digitalen Raum teilsozialisiert zu werden. Das erfordert eine Kraftanstrengung, die es aber wert sein wird.

Bildrechte: Landespolizeiamt Schleswig-Holstein.

## Literaturverzeichnis

@bremenpolizei (2021): Instagram Account. Online verfügbar unter [www.instagram.com/bremenpolizei/](https://www.instagram.com/bremenpolizei/), zuletzt aktualisiert am 22.12.2021, zuletzt geprüft am 22.12.2021.

@Polizeiberlin (2021): Instagram Account. Online verfügbar unter [www.instagram.com/polizeiberlin/](https://www.instagram.com/polizeiberlin/), zuletzt aktualisiert am 22.12.2021, zuletzt geprüft am 22.12.2021.

@polizeisachsen (2021): Instagram Account. Online verfügbar unter [www.instagram.com/polizeisachsen/](https://www.instagram.com/polizeisachsen/), zuletzt aktualisiert am 22.12.2021, zuletzt geprüft am 22.12.2021.

Bayerl, P. Saskia; Rüdiger, Thomas-Gabriel (2017): Die polizeiliche Nutzung sozialer Medien in Deutschland: Die Polizei im digitalen Neuland. In: Jürgen Stierle, Dieter Wehe und Helmut Siller (Hg.): Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis. Wiesbaden: Springer Gabler (SpringerLink Bücher), S. 919–943.

Beisch, Natalie; Koch, Wolfgang (2021): 25 Jahre ARD/ZDF-Onlinestudie: Aktuelle Aspekte der Internetnutzung in Deutschland. In: Media Perspektiven (10/2021), S. 486–503.

Bitkom (2021): Acht von zehn Personen werden Opfer von Internetkriminalität. In: Bitkom e.V., 2021. Online verfügbar unter [www.bitkom.org/Presse/Presseinformation/IT-und-Cybersicherheit-2021](https://www.bitkom.org/Presse/Presseinformation/IT-und-Cybersicherheit-2021), zuletzt geprüft am 20.12.2021.

BMI (2021a): Polizeiliche Kriminalstatistik 2020. Grundtabelle 05 - Tatschlüssel 143200. Online verfügbar unter [www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/BundFalltabellen/bundfalltabellen.html](https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/BundFalltabellen/bundfalltabellen.html).

BMI (2021b): Polizeiliche Kriminalstatistik 2020. Zeitreihe 01 - Tatschlüssel 143200. Online verfügbar unter [www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/Zeitreihen/zeitreihen\\_node.html](https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/Zeitreihen/zeitreihen_node.html).

Bodanowitz, Jörg; Scharf, Rüdiger (2020): Mediensucht 2020. Gaming und Social Media in Zeiten von Corona. DAK Forschung. Online verfügbar unter [www.dak.de/dak/gesundheit/dak-studie-gaming-social-media-und-corona-2295548.html](https://www.dak.de/dak/gesundheit/dak-studie-gaming-social-media-und-corona-2295548.html).

Bruhn, Heike; Church, Daniel; Rau, Matthias; Vogeler, Lena; Wilms, Yvonne (2021): Dritter Periodischer Sicherheitsbericht. Hg. v. Bundesministerium des Inneren, für Bau und Heimat und Bundesministerium der Justiz und für Verbraucherschutz. Online verfügbar unter [www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PeriodischerSicherheitsbericht/periodischersicherheitsbericht\\_node.html](https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PeriodischerSicherheitsbericht/periodischersicherheitsbericht_node.html).

CSAM (2021): PROJECT ARACHNID: ONLINE AVAILABILITY OF CHILD SEXUAL ABUSE MATERIAL. An analysis of CSAM and harmful-abusive content linked to certain electronic service providers. Online verfügbar unter [protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/](https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/).

Denef, Sebastian; Rüdiger, Thomas-Gabriel (2013): Soziale Medien – Muss sich die Polizei neu ausrichten? In: Deutsche Polizei 11/2013, S. 4-12.

Feierabend, Sabine; Rathgeb, Thomas; Kheredmand, Hediye; Glöckler, Stephan (2020): KIM 2020. Kindheit, Internet, Medien - Basisuntersuchung zum Medienumgang 6- bis 13-jähriger in Deutschland. Online verfügbar unter [www.mpfs.de/studien/kim-studie/2020/](http://www.mpfs.de/studien/kim-studie/2020/).

Feierabend, Sabine; Rathgeb, Thomas; Kheredmand, Hediye; Glöckler, Stephan (2021): JIM-Studie 2021. Jugend, Information, Medien. Online verfügbar unter [www.mpfs.de/studien/jim-studie/2021/](http://www.mpfs.de/studien/jim-studie/2021/).

GData (2021): Cybersicherheit – Zahl der Woche: Jede dritte Familie ist bereits einer Phishing-Mail zum Opfer gefallen. Online verfügbar unter [www.gdata.de/news/2021/12/37171-cybersicherheit-jede-dritte-familie-ist-bereits-einer-phishing-mail-zum-opfer-gefallen](http://www.gdata.de/news/2021/12/37171-cybersicherheit-jede-dritte-familie-ist-bereits-einer-phishing-mail-zum-opfer-gefallen), zuletzt aktualisiert am 20.12.2021, zuletzt geprüft am 20.12.2021.

Hoven, Elisa (2021): „Reagiert Telegram wie bisher nicht auf die deutschen Behörden, sind die derzeit möglichen juristischen Wege erschöpft“. Online verfügbar unter [nachrichten.idw-online.de/2021/12/16/reagiert-telegram-wie-bisher-nicht-auf-die-deutschen-behoerden-sind-die-derzeit-moeglichen-juristischen-wege-erschoept/](https://nachrichten.idw-online.de/2021/12/16/reagiert-telegram-wie-bisher-nicht-auf-die-deutschen-behoerden-sind-die-derzeit-moeglichen-juristischen-wege-erschoept/), zuletzt aktualisiert am 16.12.2021, zuletzt geprüft am 16.12.2021.

Konrad Adenauer Stiftung (2021): Wenn es Nacht wird in Deutschland. Ergebnisse einer repräsentativen Umfrage zu Kriminalitätsangst und der Akzeptanz von Maßnahmen gegen Kriminalität.

Krupp, Manfred; Bellut, Thomas (2021): ARD/ZDF-Onlinestudie 2021. Kompakte Präsentation. ARD ZDF. Online verfügbar unter [www.ard-zdf-onlinestudie.de/files/2021/ARD\\_ZDF\\_Onlinestudie\\_2021\\_Publikationscharts\\_final.pdf](http://www.ard-zdf-onlinestudie.de/files/2021/ARD_ZDF_Onlinestudie_2021_Publikationscharts_final.pdf).

Kuri, Jürgen (2000): Bundesregierung: Globales Strafrecht gegen Internet-Kriminalität. In: heise online, 10.05.2000. Online verfügbar unter [www.heise.de/newsticker/meldung/Bundesregierung-Globales-Strafrecht-gegen-Internet-Kriminalitaet-20444.html](http://www.heise.de/newsticker/meldung/Bundesregierung-Globales-Strafrecht-gegen-Internet-Kriminalitaet-20444.html), zuletzt geprüft am 16.12.2021.

LKA NRW (2021): Schriftliche Anhörung von Sachverständigen durch die Kommission zur Wahrnehmung der Belange der Kinder des Ausschusses für Familie, Kinder und Jugend des Landtags Nordrhein-Westfalen „Polizei und Justiz“. Stellungnahme 17/4176. Online verfügbar unter [polit-x.de/de/documents/6074495/bundeslander/nordrhein-westfalen/landtag/ausschusse/stellungnahme-2021-08-25-polizei-und-justiz-schriftliche-anhorung-der-kommission-zur-wahrnehmung-der-belange-der-kinder-des-ausschusses-fur-familie-kinder-und-jugend](https://polit-x.de/de/documents/6074495/bundeslander/nordrhein-westfalen/landtag/ausschusse/stellungnahme-2021-08-25-polizei-und-justiz-schriftliche-anhorung-der-kommission-zur-wahrnehmung-der-belange-der-kinder-des-ausschusses-fur-familie-kinder-und-jugend).

Metzger, Nils (2021): Zwischen Extremismus und Geschäftsinteresse. In: Digitales, 16.01.2021. Online verfügbar unter [www.zdf.de/nachrichten/digitales/telegram-wachstum-extremismus-werbung-100.html](http://www.zdf.de/nachrichten/digitales/telegram-wachstum-extremismus-werbung-100.html), zuletzt geprüft am 16.12.2021.

NCMEC (2021a): 2020 Reports by Electronic Service Providers (ESP).

NCMEC (2021b): Reports by Country. Online verfügbar unter [www.missingkids.org/gethelpnow/cybertipline](https://www.missingkids.org/gethelpnow/cybertipline), zuletzt aktualisiert am 02.12.2021, zuletzt geprüft am 16.12.2021.

NDR (2021): Sexuelle Gewalt gegen Kinder - wo bleibt die Hilfe? Online verfügbar unter [www.ndr.de/fernsehen/sendungen/45\\_min/Sexuelle-Gewalt-gegen-Kinder-wo-bleibt-die-Hilfe,sendung1204448.html](http://www.ndr.de/fernsehen/sendungen/45_min/Sexuelle-Gewalt-gegen-Kinder-wo-bleibt-die-Hilfe,sendung1204448.html).

Nennstiel, Sabine; Isenberg, Meike (2021): Kinder und Jugendliche als Opfer von Cybergrooming. Zentrale Ergebnisse der 1. Befragungswelle 2021. Hg. v. Landesanstalt für Medien NRW. Online verfügbar unter [www.medienanstalt-nrw.de/presse/pressemitteilungen-2021/2021/dezember/repraesentative-zahlen-zur-erfahrung-von-kindern-zwischen-8-und-18-jahren-mit-sexualisierter-ansprache-im-netz.html](http://www.medienanstalt-nrw.de/presse/pressemitteilungen-2021/2021/dezember/repraesentative-zahlen-zur-erfahrung-von-kindern-zwischen-8-und-18-jahren-mit-sexualisierter-ansprache-im-netz.html).

ProPK (2021): Kampagne gegen die Verbreitung von Kinderpornografie. Polizeiliche Kriminalprävention der Länder und des Bundes. Online verfügbar unter [www.polizei-beratung.de/themen-und-tipps/sexualdelikte/kinderpornografie/die-kampagne/](http://www.polizei-beratung.de/themen-und-tipps/sexualdelikte/kinderpornografie/die-kampagne/), zuletzt aktualisiert am 16.12.2021, zuletzt geprüft am 16.12.2021.

Rüdiger, Thomas-Gabriel (2019): Haben wir eine Unrechtskultur im digitalen Raum? In: Kriminalistik (01/2019), S. 37-43.

Rüdiger, Thomas-Gabriel (2020): Die onlinebasierte Anbahnung des sexuellen Missbrauchs eines Kindes: Verlag für Polizeiwissenschaft.

Rüdiger, Thomas-Gabriel (2021): Digitale Kriminalitätstransparenz. Von der Durchbrechung der „Präventivwirkung des Nichtwissens“. In: Kriminalistik (2/2021), S. 72–78.

Statistisches Bundesamt (2021): Bevölkerung nach Nationalität und Geschlecht (Quartalszahlen). Online verfügbar unter [www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/Tabellen/liste-zensus-geschlecht-staatsangehoerigkeit.html;jsessionid=FA2E4D117DF817E8C8305732F61D8851.live711](https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/Tabellen/liste-zensus-geschlecht-staatsangehoerigkeit.html;jsessionid=FA2E4D117DF817E8C8305732F61D8851.live711), zuletzt aktualisiert am 07.07.2021, zuletzt geprüft am 11.11.2021.

Welle, Deutsche (2021): BKA: Kinderpornografie massiv gestiegen | DW | 07.11.2021. Deutsche Welle (www.dw.com). Online verfügbar unter [www.dw.com/de/bka-kinderpornografie-massiv-gestiegen/a-59747468](https://www.dw.com/de/bka-kinderpornografie-massiv-gestiegen/a-59747468), zuletzt aktualisiert am 10.11.2021, zuletzt geprüft am 10.11.2021.

---

## Anmerkungen

---

\* Dr. iur. Thomas-Gabriel Rüdiger M.A. ist Akademischer Oberrat und Leiter des Instituts für Cyberkriminologie an der Hochschule der Polizei des Landes Brandenburg. Aufgrund des Redaktionsschlusses des Artikels finden nur die Fallzahlen bis zur PKS 2020 Berücksichtigung.